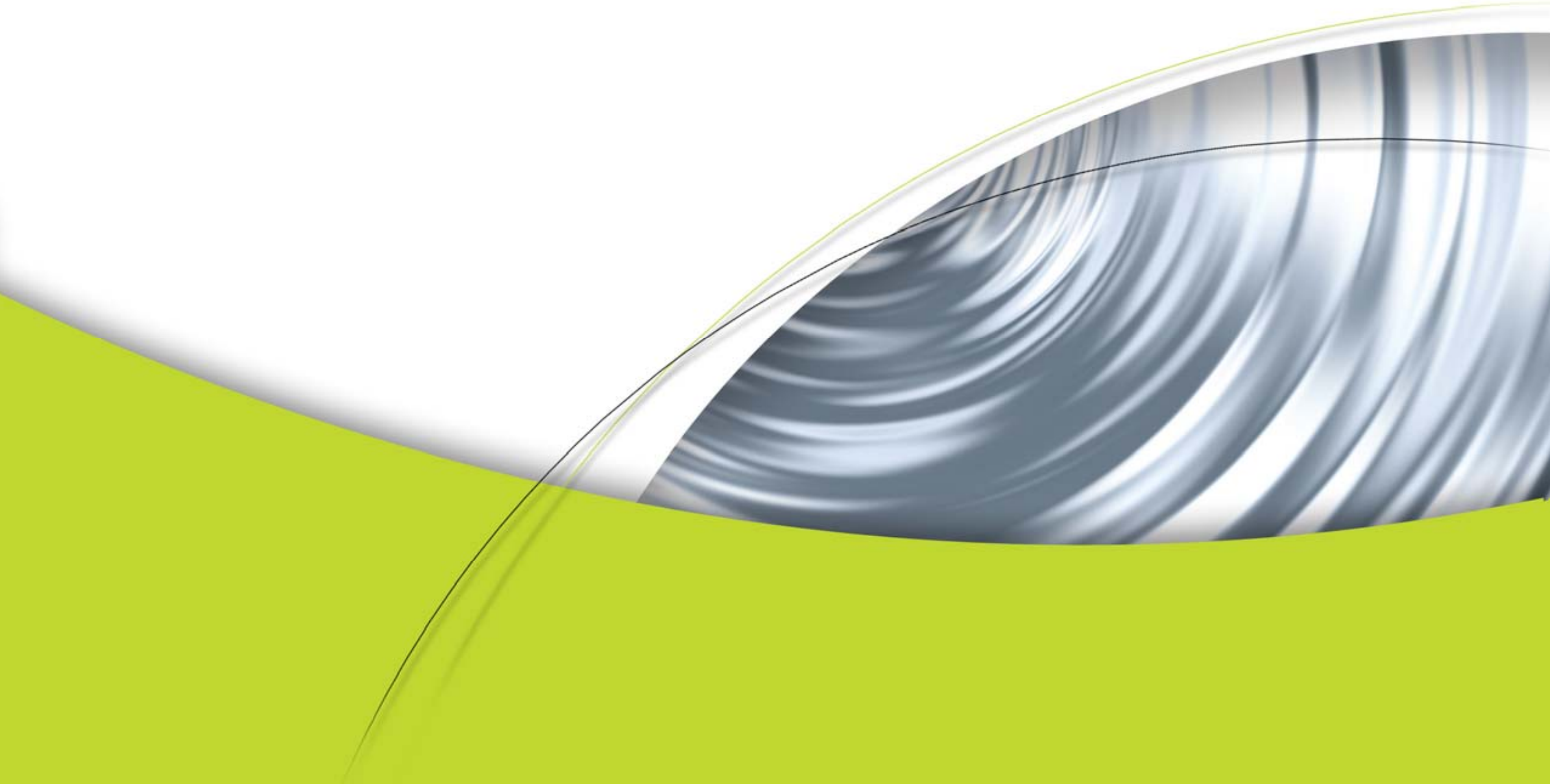
Quick Start Guide

NVIDIA Firewall and ActiveArmor

Quick Start Guide



Quick Start Guide for NVIDIA Firewall and ActiveArmor

Basic Security Concepts

There are two components for NVIDIA security solutions:

- NVIDIA Firewall
- NVIDIA ActiveArmor Secure Network Engine

NVIDIA Firewall:

NVIDIA Firewall—the only *native* firewall in the market—is optimized and integrated into the NVIDIA nForce systems that support ForceWare Network Access Manager. The NVIDIA Firewall is a high performance, *hardware-optimized* firewall offering enhanced reliability and protection at the end-point—i.e., the desktop. It incorporates firewall and antihacking technologies such as anti-spoofing, anti-sniffing, anti-ARP cache poisoning, and anti-DHCP server, which are important security controls for corporate network environments.

ActiveArmor:

NVIDIA ActiveArmor is software that controls the NVIDIA ActiveArmor Secure Networking Engine (SNE), which offloads CPU-intensive aspects of firewall and TCP processing. By processing the packets of those connections that are offloaded, the SNE significantly reduces CPU usage and accelerates firewall throughput.

The ActiveArmor offloading policy is defined using the Web-based Network Access Manager (NAM), and configuring ActiveArmor is similar to the process used for the NVIDIA Firewall.

By default, ActiveArmor is enabled whenever the NVIDIA Firewall is installed; however, ActiveArmor is not configured to offload any connections from the NVIDIA Firewall. You must define a policy that controls which connections are offloaded to ActiveArmor (and which are not).

Before Using the ForceWare Network Access Manager Installer

Before you run the ForceWare Network Access Manager installer program, `NetworkAccessManagerSetup.exe`, note the following:

- ❑ The nForce Ethernet driver must already be installed and operational on your computer.
- ❑ You must have Administrator access rights to do the following:
  - ➢ Run the Setup installation program.
  - ➢ Uninstall and/or modify the ForceWare Network Access Manager software, as needed.
- ❑ If you are using the ForceWare Network Access Manager Web-based interface, note the following:
  - ➢ Microsoft Internet Explorer version 5 or later must be running on your computer.
  - ➢ The ForceWare Network Access Manager Web-based interface uses the NVIDIA registered TCP port 3476. Make sure no other network application uses port 3476.

Installing ForceWare Network Access Manager

There are two ways to install the Network Access Manager (NAM)

- ❑ Locate the NetworkAccessManagerSetup.exe on the CD that you might have received or from the web site that you might have downloaded the software
- ❑ Or Run the main installer and select the network components that you want to install

Launching the ForceWare Network Access Manager Web Interface

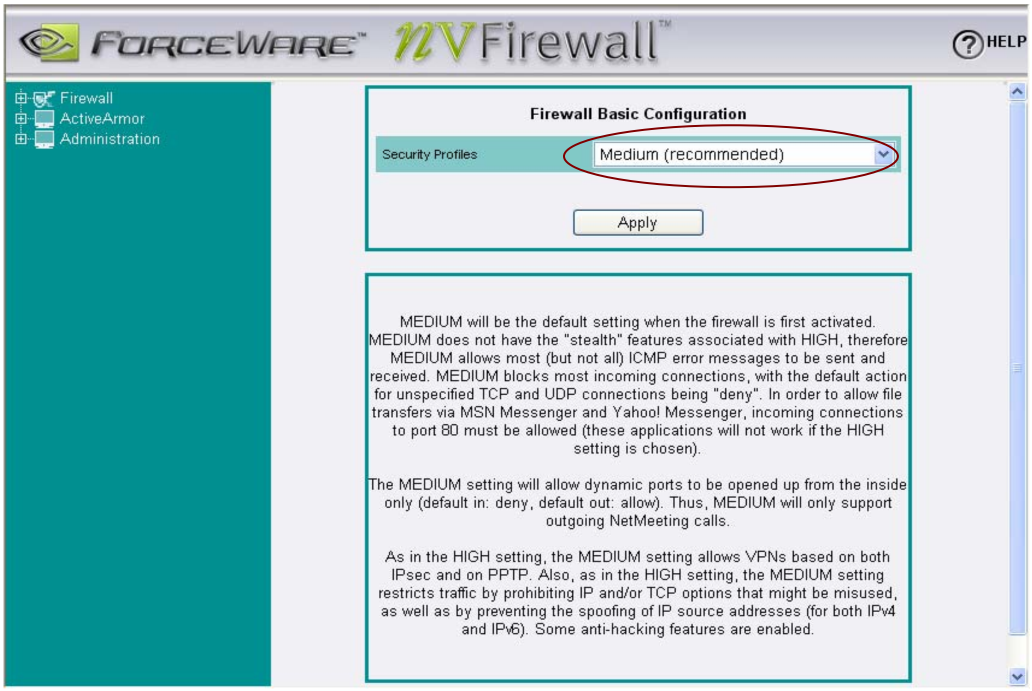
To launch the ForceWare Network Access Manager Web-based interface, click the following from your Windows taskbar:
Start→Programs→ NVIDIA Corporation→Network Access Manager→Web-based Interface.

To launch *just* the NVIDIA Firewall Web interface, click the following from your Windows taskbar :
Start→Programs→NVIDIA Corporation→Network Access Manager→NVIDIA Firewall.

The NVIDIA Firewall Web interface allows you to configure the NVIDIA Firewall, ActiveArmor, and other general administrative features.

Basic Firewall Operations

Assuming that the NVIDIA Firewall is installed, configured properly, and turned on, the following opening screen should be displayed:



Firewall Basic Configuration

Security Profiles: Medium (recommended)

MEDIUM will be the default setting when the firewall is first activated. MEDIUM does not have the "stealth" features associated with HIGH, therefore MEDIUM allows most (but not all) ICMP error messages to be sent and received. MEDIUM blocks most incoming connections, with the default action for unspecified TCP and UDP connections being "deny". In order to allow file transfers via MSN Messenger and Yahoo! Messenger, incoming connections to port 80 must be allowed (these applications will not work if the HIGH setting is chosen).

The MEDIUM setting will allow dynamic ports to be opened up from the inside only (default in: deny, default out: allow). Thus, MEDIUM will only support outgoing NetMeeting calls.

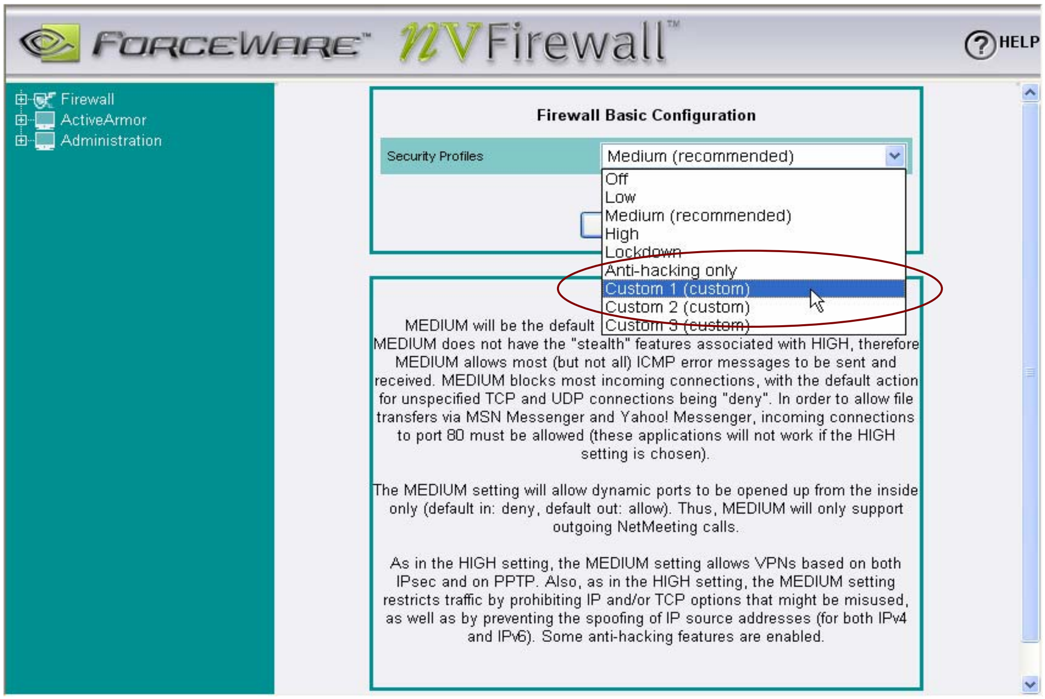
As in the HIGH setting, the MEDIUM setting allows VPNs based on both IPsec and on PPTP. Also, as in the HIGH setting, the MEDIUM setting restricts traffic by prohibiting IP and/or TCP options that might be misused, as well as by preventing the spoofing of IP source addresses (for both IPv4 and IPv6). Some anti-hacking features are enabled.

Figure 1. NVFirewall Opening Screen

When the firewall is turned on for the first time, it defaults to **Medium** profile, as shown in Figure 1. The **Medium** profile is a good balance between security and functionality. That means, your PC is protected from the most common attacks, while at the same time the majority of your applications function without having the user configure the firewall. This is the recommended method of operation for most users.

When the firewall is set to **Medium** profile, you can not add ports, delete ports or change any settings such as enable or disable certain Anti-Hacking features. Again, all firewall settings are set and can not be changed. If you want to change the default settings, then you must create a *custom profile*. A custom profile provides full access to all the firewall's functionality and the can change the behavior of the firewall in any way you wants.

To change a profile, click on the active profile (in this example the active profile is **Medium (recommended)**) then select **Custom 1** as shown in Figure 2.



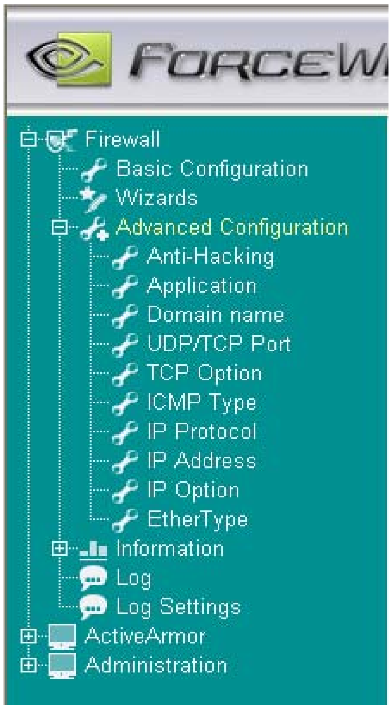
MEDIUM will be the default

MEDIUM does not have the "stealth" features associated with HIGH, therefore MEDIUM allows most (but not all) ICMP error messages to be sent and received. MEDIUM blocks most incoming connections, with the default action for unspecified TCP and UDP connections being "deny". In order to allow file transfers via MSN Messenger and Yahoo! Messenger, incoming connections to port 80 must be allowed (these applications will not work if the HIGH setting is chosen).

The MEDIUM setting will allow dynamic ports to be opened up from the inside only (default in: deny, default out: allow). Thus, MEDIUM will only support outgoing NetMeeting calls.

As in the HIGH setting, the MEDIUM setting allows VPNs based on both IPsec and on PPTP. Also, as in the HIGH setting, the MEDIUM setting restricts traffic by prohibiting IP and/or TCP options that might be misused, as well as by preventing the spoofing of IP source addresses (for both IPv4 and IPv6). Some anti-hacking features are enabled.

Figure 2. Configuring the Firewall



Next, expand the **Firewall** list located in the left blue window of the screen. Expand **Advanced Configuration** to display the Advanced Configuration list of options

Anti-Hacking: These are features designed to protect your PC from some of the most common hacking attacks. The anti-hacking features of the NVIDIA Firewall include anti-spoofing, anti-sniffing, anti-ARP cache poisoning, and anti-DHCP server, all of which Provide an advanced level of protection.

Application: This is the table used by the Intelligent Application Manager (IAM) to track which application is allowed or denied network access.

Domain name: This is where the user can configure the firewall to block or allow access to certain domain names and web sites. It provides a basic level of web filtering.

UDP/TCP port: This is where a user can configure which ports are open or closed both either inbound or outbound connections.

TCP Options: This section is for advanced uses who want to do filtering based on the TCP Options such as Window Scale.

ICMP Type: This deals with management traffic access control such as Ping.

IP Protocol: This section is for advanced uses who want to do filtering based on IP Protocols such as GRE.

IP Address: Basic filtering based on IP address and subnet mask.

IP Options: This section is for advanced uses who want to do filtering based on the IP Options Time Stamp.

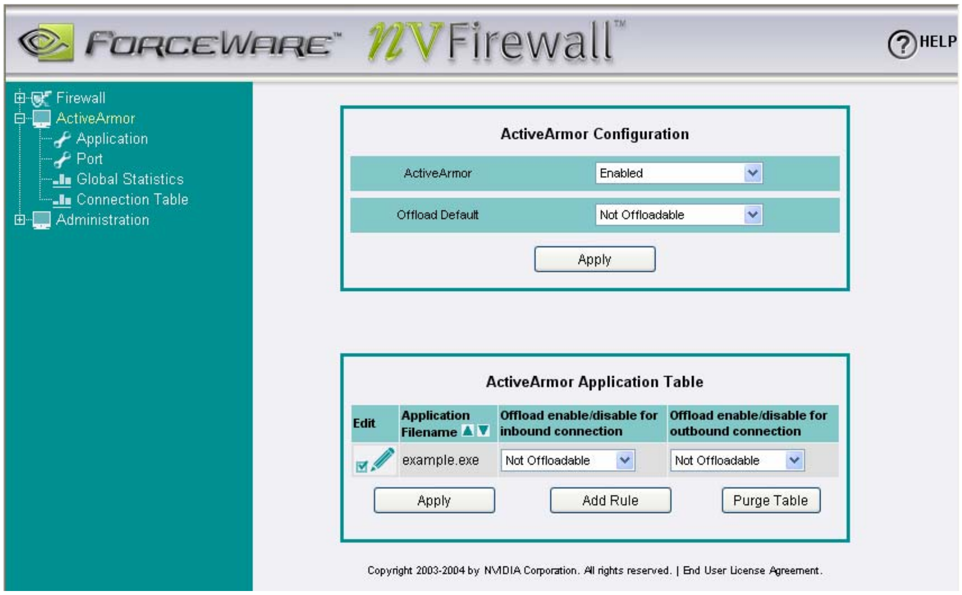
EtherType: This section is for advanced uses who want to do filtering based on EtherType such as PPPoE.

The NVIDIA Firewall also has extensive monitoring capabilities (monitors all inbound and outbound traffic, both allowed and denied), as well as logging capabilities which can be exported to a text file for analysis.

ActiveArmor

ActiveArmor is automatically turned off and on with the NVIDIA Firewall. However, it is possible to manually turn on ActiveArmor without the Firewall being on.

Expand **ActiveArmor** and click on **Application** to display the ActiveArmor Configuration screen (Figure 3):



ActiveArmor Configuration

ActiveArmor	Enabled
Offload Default	Not Offloadable

Apply

ActiveArmor Application Table

Edit	Application Filename	Offload enable/disable for inbound connection	Offload enable/disable for outbound connection
☑	example.exe	Not Offloadable	Not Offloadable

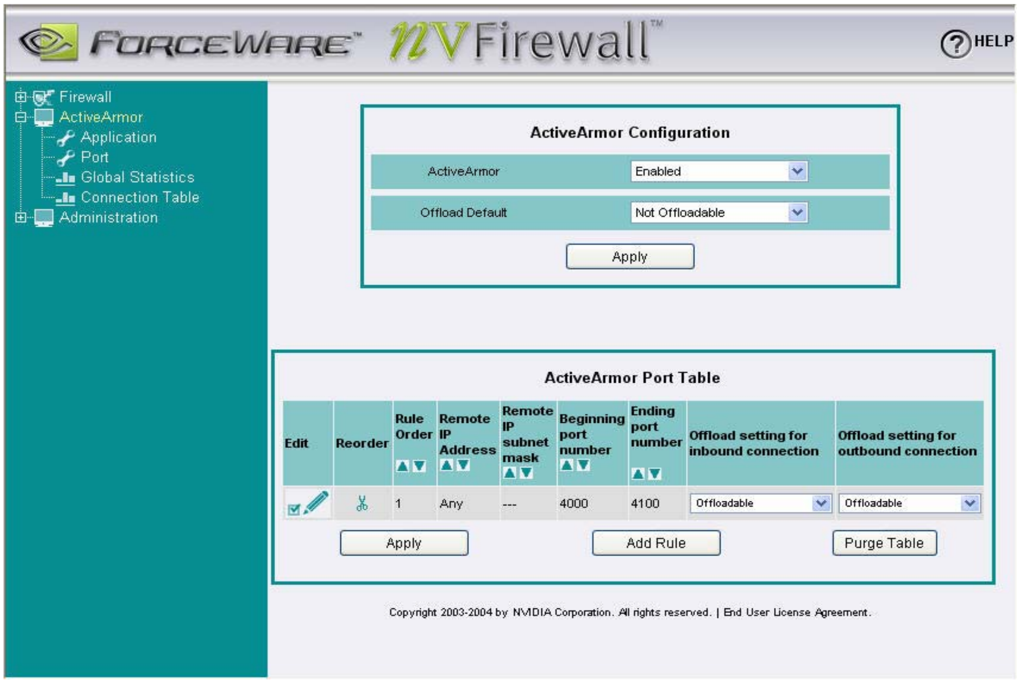
Apply Add Rule Purge Table

Copyright 2003-2004 by NVIDIA Corporation. All rights reserved. | End User License Agreement.

Figure 3. ActiveArmor Configuration Screen

As shown in Figure 3, ActiveArmor is **Enabled**. ActiveArmor can be enabled or disabled regardless of the status of the firewall.

You can specify which applications (which ports) can be offloaded (calculations done in hardware). In order to do that, click on **Port** to display the ActiveArmor Port Table in the lower portion of the screen (as shown in Figure 4).



ActiveArmor Configuration

ActiveArmor: Enabled

Offload Default: Not Offloadable

ActiveArmor Port Table

Edit	Reorder	Rule Order	Remote IP Address	Remote IP subnet mask	Beginning port number	Ending port number	Offload setting for inbound connection	Offload setting for outbound connection
☑ ✎	✂	1	Any	---	4000	4100	Offloadable	Offloadable

Copyright 2003-2004 by NVIDIA Corporation. All rights reserved. | End User License Agreement.

Figure 4. ActiveArmor Port Table

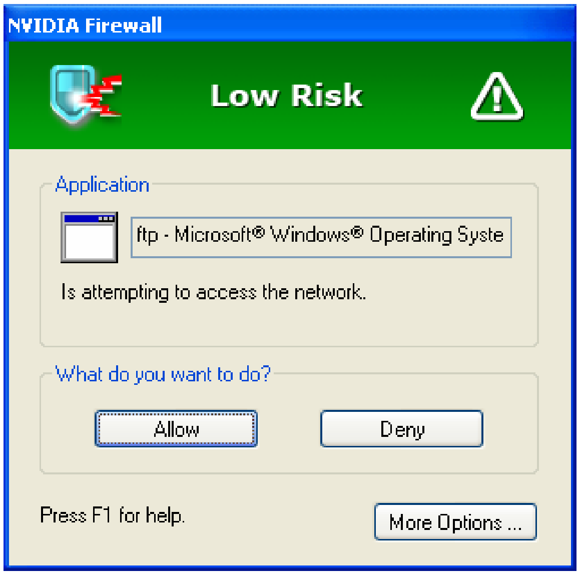
As shown in Figure 4, an application has been added that uses ports between 4000 and 4100 to be offloaded.

You can also monitor how many packets were offloaded and various other statistics by click on **Global Statistics**. Similarly, you can monitor the active offloaded connections by click on **Connection Table**.

Intelligent Application Manager

The Intelligent Application Manager (IAM) allows you to create firewall rules based on an application's name. When an application attempts to open a new network connection (either as a client or as a server), you are prompted by a pop-up dialog to either allow or deny the application's access to the network. An application-based firewall rule is then automatically created or modified based on your decision. Applications can be allowed or denied on the fly by you, and you have the ultimate control over whether an unknown application can or cannot access the network. Filtering by ports is also available; augmenting the more user-friendly filtering based on application names the IAM provides in the NVIDIA Firewall.

Assuming a user is trying to establish an FTP connection from his machine to a remote FTP server, IAM intercepts such an activity and the following prompt is displayed:

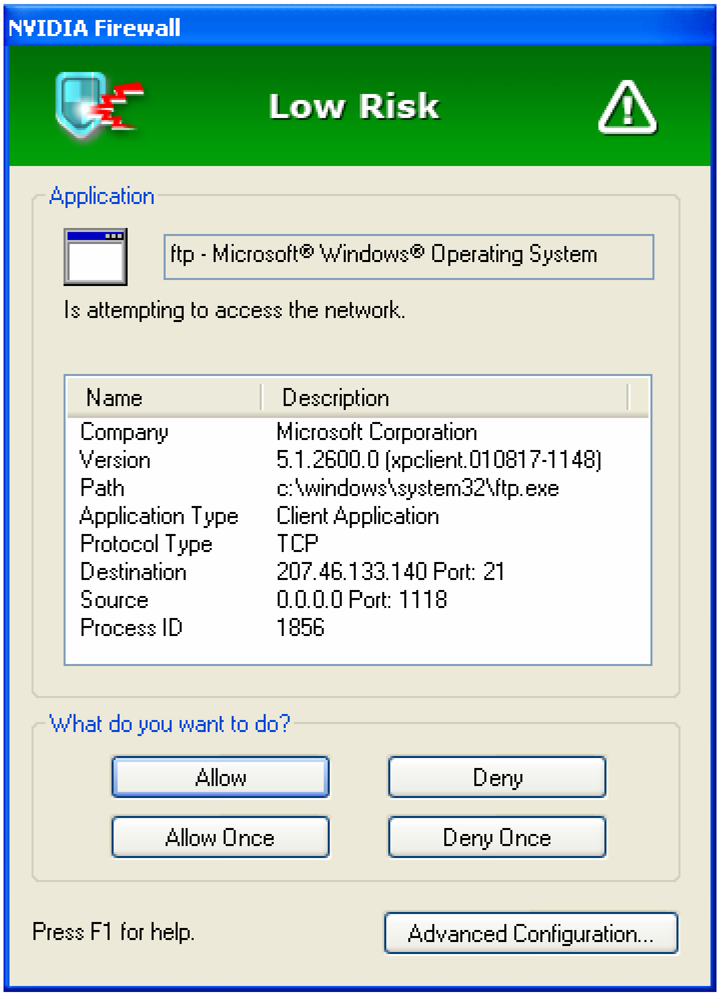


ftp - Microsoft® Windows® Operating Syste

Is attempting to access the network.

Allow means allow always, while **Deny** means deny always (never prompt again). To get more detailed information, click **More Options...** to display the screen shown in Figure 5.

Note that the IAM prompt windows displays if the application is **Low**, **Medium**, or **High Risk**. IAM also dynamically opens the proper ports for the most commonly used application and services by Windows without prompting the user.



ftp - Microsoft® Windows® Operating System

Is attempting to access the network.

Name	Description
Company	Microsoft Corporation
Version	5.1.2600.0 (xpclient.010817-1148)
Path	c:\windows\system32\ftp.exe
Application Type	Client Application
Protocol Type	TCP
Destination	207.46.133.140 Port: 21
Source	0.0.0.0 Port: 1118
Process ID	1856

Press F1 for help.

Figure 5. Nvidia Firewall IAM Options

Notice

ALL NVIDIA DESIGN SPECIFICATIONS, REFERENCE BOARDS, FILES, DRAWINGS, DIAGNOSTICS, LISTS, AND OTHER DOCUMENTS (TOGETHER AND SEPARATELY, “MATERIALS”) ARE BEING PROVIDED “AS IS." NVIDIA MAKES NO WARRANTIES, EXPRESSED, IMPLIED, STATUTORY, OR OTHERWISE WITH RESPECT TO THE MATERIALS, AND EXPRESSLY DISCLAIMS ALL IMPLIED WARRANTIES OF NONINFRINGEMENT, MERCHANTABILITY, AND FITNESS FOR A PARTICULAR PURPOSE.

Information furnished is believed to be accurate and reliable. However, NVIDIA Corporation assumes no responsibility for the consequences of use of such information or for any infringement of patents or other rights of third parties that may result from its use. No license is granted by implication or otherwise under any patent or patent rights of NVIDIA Corporation. Specifications mentioned in this publication are subject to change without notice. This publication supersedes and replaces all information previously supplied. NVIDIA Corporation products are not authorized for use as critical components in life support devices or systems without express written approval of NVIDIA Corporation.

Trademarks

Copyright

NVIDIA Corporation
2701 San Tomas Expressway
Santa Clara, CA 95050
www.nvidia.com